

## REMARKS

### A. Background

Claims 1-4, 6-13, and 15-18 were pending in the application at the time of the Office Action. Claims 1-4, 6-13, and 15-18 were rejected as being obvious over cited prior art. By this response applicant has amended the specification and drawings for purposes of technical accuracy. Applicant has also amended claims 1-4, 6-13, 15-16, and 18 and added new claims 19-25. As such, claims 1-4, 6-13, and 15-25 are presented for the Examiner's consideration in light of the following remarks.

### B. Proposed Amendments

#### 1. Specification

Applicant presents a replacement title for the application. Applicants have amended the title of the invention to more precisely refer to the subject matter of the invention. In view of the foregoing, Applicant respectfully submits that the amendment to the specification does not introduce new matter and entry thereof is respectfully requested.

#### 2. Drawings

To facilitate the Examiner's consideration and approval of the proposed drawings changes, a Replacement Sheet containing Figure 4 and an Annotated Marked-up Drawing containing Figure 4 and showing the changes therein are being transmitted herewith. The drawing amendments are presented for purposes of technical accuracy and consistency with respect to the meaning of the term "encryption" used herein. These amendments are fully consistent with the original specification and the ordinary knowledge of persons skilled in the art, and do not add new matter.

In view of the foregoing, Applicant respectfully submits that the amendments to the drawings do not introduce new matter and entry thereof is respectfully requested.

2. Claims

Please amend the claims in the manner indicated above, where an underline represents new text, and strikeouts are used to indicate deleted text. The amendments to claim 1-4, 6-13, 15-16, and 18, as well as new claims 19-22 are fully supported in the specification as originally filled. Applicants have amended the claims, as a whole, to correct or improve upon language therein and these changes are believed to be self-evident on the face of the foregoing. The words “encoding” and “decoding” in the preamble to the claims have been removed for the same reason as the aforesaid title amendment. In addition, these words have been removed from the references to encryption and decryption for purposes of technical accuracy and consistency.

New dependent claims 19-22 and 24-25 have been added to define additional inventive features described in, and supported by, the specification. No new matter is added by these new claims.

New independent claim 23 has been added to sufficiently and patentably define a broadest aspect of Applicants’ invention. No new matter is added by this new claim.

In view of the foregoing discussion, applicant submits that the amendments to the claims do not introduce new matter and entry thereof is respectfully requested.

C. Rejection on the Merits

Paragraphs 4 and 5 of the Office Action rejected claims 1-4, 6-13, and 15-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,708,717 to *Alasia* in view of U.S. Patent No. 6,104,812 to *Koltai et al.*

Applicants have reviewed the Examiner's comments in the Office Action dated 19 October, 2004 from which it is apparent that some confusion or misunderstanding has occurred, by the Examiner, with respect to what is actually contained in, and taught by, the cited prior art. This confusion or misunderstanding appears to have possibly arisen by reason of the misuse of certain, well-known technical terms by *Alasia*, as detailed more fully below.

Specifically, the Examiner has confused: (I) the meaning of certain well-known technical terms which are misused in the prior art; and, in turn, (II) the fundamental features of the invention defined by the amended claims. More specifically:

I. The Examiner has confused the terms “encoding”, “deflection encoding” and “encryption”, as evidenced on page 5 of the Office Action, line 14, in which the Examiner (wrongly) states: “(i.e. “encryption encoding” same as “scramble latent images”)”; and,

II. The Examiner has confused, or misunderstood:

(i) The prior art processes which apply one or more single-level encoding steps (i.e. an optical “scrambling” only) to one or more target images to hide (i.e. optically disguise) those image(s) within a visible image, and thereby produce a single-level decodable hidden image as a security feature; as compared to,

(ii) Applicants' process of applying two independent, different-level encoding steps (i.e. optical, deflection encoding at one level and mathematical encryption at a higher level) to two different images (viz. to a source image and a

deflected image or, alternatively, to two sources images), to completely transform those images (not simply hide them within a visible image), and thereby produce two independently, different-level decodable images as a unitary security feature, either or both of which can be selected for decoding by a user without interference with the other (the optical level security feature being decodable by optical decoding and the mathematical level security feature being decodable by decryption).

#### **I. The meaning of “encryption” / “decryption”:**

The terms “encryption” and “decryption” are defined to mean a high-level encoding/decoding process which applies a unique mathematical encryption key to data such that only the data provider controlling the encryption process has knowledge of that unique key and, thus, only the data provider has control over access to that data and the means required to decrypt that encrypted data. Examples of encryption include RSA and DES. Encryption, unlike low-level types of encoding (examples of which are Morse code and UPC bar codes), allows only the authorized recipients to access the data. The meaning of “encoding”, as generally covering low-level types of encoding, is contrasted with the specific meaning of encryption in the “Web Dictionary of Cybernetics and Systems”, published at the Internal URL <http://pespmc1.vub.ac.be/ASC/indexASC.html>, which is a combination of the ASC Glossary, Krippendorff’s Dictionary and Hornung’s Glossary and is well-known and regarded to be accurate and reliable:

*Conversion of plaintext into encoded data by using a code which need not be secret, in contrast to encryption. This conversion is done in such a way that reversion into the original form is possible by decoding. In contrast to encrypted data encoded data may well be understandable by someone who knows well enough the code (e.g. ICD code, morse code, ASCII code etc.). (Hornung).*

Similarly, the following definition of the term “encryption” is a standard adopted within the Internet Security Glossary of the Network Working Group, Internet Society (www.isoc.org), published as RFC 2828, May, 2000 at Internet URL <ftp://ftp.rfc-editor.org/in-notes/rfc2828.txt>:

*Encryption*

*(C) Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are **control parameters**: (a) a key value that varies the transformation and, in some cases, (b) an initialization value that establishes the starting state of the algorithm.*

**II. Confusion between prior art security processes and applicants’ claimed invention:**

The terms “encode” and “decode” may be used to refer generally to security processing but the terms “deflection encoding” and “encryption”, as used in applicants’ independent claims 1, 10 and 23, specifically define a particular low-level-type optical security process and a particular high-level-type mathematical security process, respectively. By contrast, the cited prior art contemplates one-only, low-level-type security process which may be applied once ( per *Alasia*’s one-phase S.I. operation, see column 6, lines 49-51) or on a repeated basis (per *Alasia*’s two- and three-phase S.I. operations, see column 10, line 59 to column 11, line 8). Encryption is not contemplated by any of the cited references. Further, none of the cited references in any manner contemplates the unitary security feature of claims 1, 10 and 23 which provides two, independently solvable indicia of which one is solvable using a low-level deflection decoding process while the other is solvable only through a high-level decryption process.

The cited patent to *Alasia* incorrectly uses the terms “encrypted”, “encoded” and “scrambled” interchangeably but it is clear from *Alasia* that the only process used is that of optical “scrambling” (a form of optical encoding resulting in “Scrambled Indicia (S.I.)”) and that a “lenticular decoder

lens” (i.e. an optical lens for decoding such S.I.) is required by *Alasia* (see column 6, lines 33-47).

The Examiner’s following interpretations of *Alasia* are incorrect:

-on page 5 of the Office Action, the Examiner’s allegation that *Alasia* satisfies the claim feature “*whereby neither of said first and second said source images is visible upon viewing said security device image*” is incorrect. In fact, the whole purpose and processing of *Alasia* (and *Koltai* which teaches the same, for present purposes) is to hide one (or more) images, alternately referred to by *Alasia* as “scrambled” and “latent” images, within a visible source image (see column 6, lines 31-47, column 8 lines 62-67 to column 9, lines 1-5 and column 11, lines 60-67 to column 12, lines 4-14). In making this allegation, it appears that the Examiner is not comparing the resulting printable, security device image of *Alasia* but, rather, is focusing on the pre-processing of the hidden image (only) of *Alasia*;

-on page 6 of the Office Action, the Examiner’s allegation that *Alasia* satisfies the claim feature “*and wherein each of said deflected and encrypted images is preserved and identifiable by means of a predetermined feature such that either of said deflected and encrypted images may be decoded without interfering with an ability to separately decode the other of said deflected and encrypted images*” is incorrect. Firstly, neither *Alasia* nor any of the other cited references provides either of the claimed deflected and encrypted images. Secondly, neither *Alasia* nor any of the other cited references discloses, teaches or in any way suggests preserving both a deflected image and an encrypted image within a printable security device image such that each may be decoded without interfering with an ability to separately decode the other. To support this allegation, the Examiner seeks to rely upon the option taught by *Alasia* to use two-phase S.I. scrambling, or three-phase S.I. scrambling, but each of these applies the same optical encoding process of the one-phase S.I. scrambling, but

in repetition. That is, such multi-phase scrambling steps merely serve to scramble and combine multiple images into one scrambled image which is then itself hidden in a visible image in the same manner as the one-phase SI operation (see column 6, lines 48-51 and Figure 1 and also column 2, lines 39-48 and column 10, line 59 to column 11, line 8); and,

-on page 7 of the Office Action the Examiner's allegation that *Alasia* satisfies the claim feature "(ii) computer decoding processing applying said software lense to said deflected image, each said decoding means being selectable according to a user's choice without interference from any prior use of either or both said decoding means to detect said first source image and said encrypted image is configured for detecting therefrom either said deflected image or said second source image by means of computer decoding processing applying a decryption function corresponding to said encryption function to said encrypted image" is incorrect. Neither *Alasia* nor any of the cited references discloses or in any manner suggests any such separate (independent) encrypted image provided as a second, high-level security layer, and which is decrypted using a decryption function to detect either the deflected image or second source image (depending on which of those images was encrypted by the encryption processing).

*Koltai* is very similar to *Alasia*. Like *Alasia*, *Koltai* "encodes" screens to hide a secondary image within a primary image using the well-known concept of steganography and the hidden image is extracted either optically or electronically (*Koltai* simply adds some digital processing so that some electronic decoding is required to detect that same hidden image). Like the other cited prior art, *Koltai* not disclose or in any way suggest a further encryption layer of security that is independently solvable, such as that provided by applicants' claimed security device image.

By contrast, applicants' system (and method) for producing a security device image encodes a source image by deflection encoding - i.e. transforms that source image into an array of deflected lines by computer means whereby the transformation is referred to as a "deflected image" - and then effectively adds to that deflected image a second, independent encrypted image which is itself a high-level mathematical transformation of a selected image, with neither the source nor selected images being visible in the resulting security device image.

Since the combination of *Alasia* and *Koltai* does not teach or suggest all of the elements claimed in independent claims 1 and 10, a case of *prima facie* obviousness has not been made. Additionally, claims 2-4, 6-9, 11-13 and 15-18 depend from independent claims 1 and 10, and thus incorporate the limitations thereof. As such, Applicant submits that claims 2-4, 6-9, 11-13 and 15-18 are distinguished over *Alasia* and *Koltai* for at least the same reasons as discussed above with regard to claims 1 and 14. Accordingly, it is submitted that, the cited references do not render obvious the subject matter of any of the present claims and this is true, whether the reference is considered alone or in combination with other prior art. In view of the present claim amendments and the foregoing submissions, reconsideration and withdrawal of the obviousness rejection is respectfully requested.

Paragraph 6 of the Office Action rejected claims 6-9 and 15-18 under 35 USC § 103(a) as being unpatentable over the *Alasia* patent in further view of the *Koltai* patent and further in view of U.S. Patent No. 5,303,370 to *Brosh et al.*

For the sake of brevity, the above-discussion pertaining to *Alasia* and *Koltai* is assumed to be included herein by reference. As such, Applicant respectfully asserts that the addition of *Brosh* does not include the aforementioned defects of *Alasia* and *Koltai*. As for *Alasia*, the cited patent to *Brosh* misuses the term "encrypted" and it is clear that the hidden images of *Brosh* are constituted by an optical encoding process and reconstituted by an optical process (see column 4, line 21-25). *Brosh*



does not disclose or in any way suggest a further encryption layer of security that is independently solvable, such as that provided by applicants' claimed security device image.

Since the combination of *Alasia*, *Koltai*, and *Brosh* does not teach or suggest all of the elements claimed in claims 6-9 and 15-18, a case of *prima facie* obviousness has not been made. Accordingly, it is submitted that, the cited references do not render obvious the subject matter of any of the present claims and this is true, whether the reference is considered alone or in combination with other prior art. In view of the present claim amendments and the foregoing submissions, reconsideration and withdrawal of the obviousness rejection is respectfully requested.

D. New Claims

Applicant has added new claims 19-25, which are fully supported by the specification as originally filed. As such, the new claims set forth the subject matter Applicant claims as the invention. Moreover, Applicants' system defined by claim 19 further provides means for personalizing the security device image to the particular document onto which it is printed, namely, using a personal identifying feature of the document (e.g. an identification number) in the encryption function. No such personalization feature in the security device image is disclosed in the prior art.

Also, Applicants' method defined by claim 22 provides further means for personalizing the security device image to the particular document onto which it is printed, namely, defining the software lens by a parameter which is determined by pre-selected identifying data associated with that document. No such personalization feature in the security device image is disclosed in the prior art.

Accordingly, it is submitted that, the cited references do not render obvious the subject matter of any of the new claims and this is true, whether the reference is considered alone or in combination with other prior art.

E. Conclusion

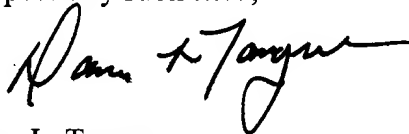
Applicant notes that this response does not discuss every reason why the claims of the present application are distinguished over the cited prior art. Most notably, Applicant submits that many if not all of the dependent claims are independently distinguishable over the cited prior art. Applicant has merely submitted those arguments which it considers sufficient to clearly distinguish the claims over the cited prior art.

In view of the foregoing, Applicant respectfully requests the Examiner's reconsideration and allowance of claims 1-4, 6-13, and 15-25 as amended and presented herein.

In the event there remains any impediment to allowance of the claims which could be clarified in a telephonic interview, the Examiner is respectfully requested to initiate such an interview with the undersigned.

Dated this 18<sup>th</sup> day of February 2005.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Dana L. Tangren', with a stylized flourish at the end.

Dana L. Tangren  
Attorney for Applicant  
Registration No. 37,246  
Customer No. 022913  
Telephone No. 801.533.9800

DLT:JMB:dfw  
W:\135872\DFW0000013074V001.DOC

## **DRAWING AMENDMENTS**

The attached drawing sheets include changes to Figure 4. The attached “Replacement Sheet,” which includes Figure 4, replaces the original sheet including Figure 4. Additionally, the “Annotated Marked-up Drawing” sheet is a marked-up copy of Figure 4 showing the amendments and annotations. In the replacement sheet for Figure 4, previously included elements “Encoding function generator” and “Encoding module” have been replaced with “Encryption function generator” and “Encryption module,” respectively.

Attachment: Replacement Sheet and Annotated Marked-up Drawing

TITLE: SYSTEM FOR IMAGE ENCODING AND DECODING AND THE PRINTABLE SECURITY  
DEVICE PRODUCED THEREFROM

Serial No. 09/553,454

Docket No. 13587.2

Annotated Sheet

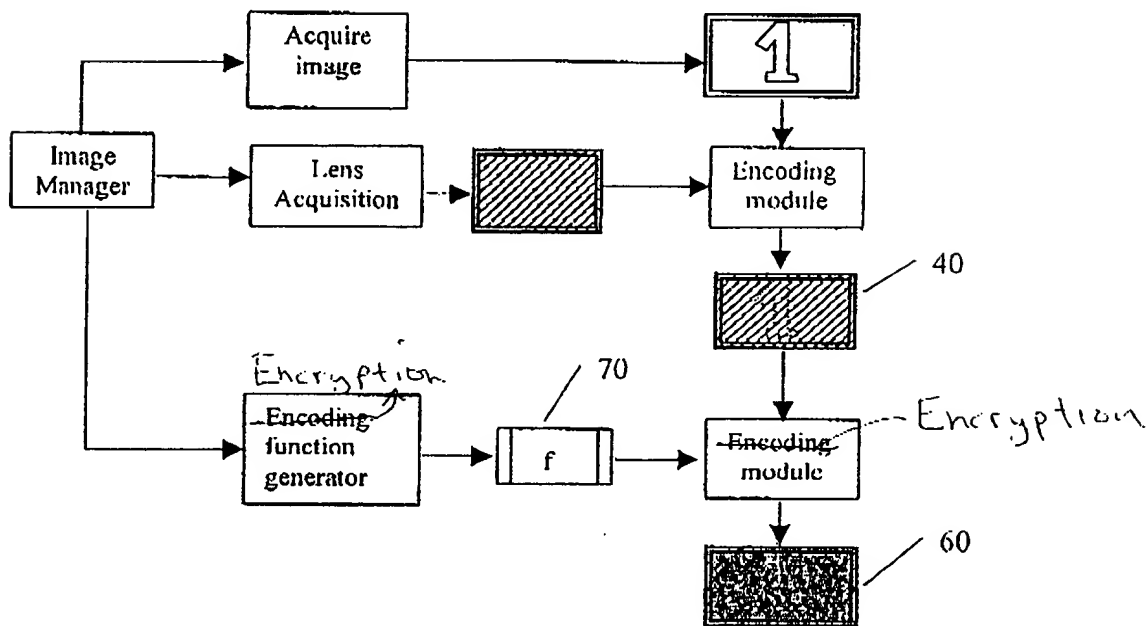


Figure 4